

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with the Apple ID
jwellz1987@gmail.com and DSID 11069587135 that is
stored at premises controlled by Apple Inc.

Case No.

3:18 mj 756

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment Alocated in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

See Attachment C

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig
Applicant's Signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 11-21-18

City and state: Dayton, Ohio

Sharon L. Ovington
Judge's signature

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Information associated with the Apple ID jwellz1987@gmail.com and DSID **11069587135** that is stored at premises controlled by Apple Inc., a company that accepts service of legal process at 1 Infinite Loop, Cupertino, California, 95014.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);
- g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;
- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Pursuant to the warrant, Apple Inc. shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of child pornography) and 18 U.S.C. §§ 2252(a) and (e) (production of child pornography) from January 1, 2016 through the present, including but not limited to the following:

- a. Any visual depictions and records related to the possession and production of child pornography;
- b. Any visual depictions of minors;
- c. Any Internet history indicative of searching for child pornography;
- d. Any Internet or cellular telephone communications (including text messages, email, social media, and online chat programs) with others in which child exploitation materials and offenses are discussed and/or traded, and any contact / identifying information for these individuals;
- e. Any Internet or electronic telephone communications (including text messages, email, social media chat programs, and online chat programs) with minors, and any contact / identifying information for these minors;
- f. Evidence of utilization of text messages, email accounts, social media accounts, online chat programs, and Peer-to-Peer file sharing programs, including any account / user names;
- g. Any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by the Apple accounts listed in Attachment A;
- h. Any GPS information accessed by the Apple accounts listed in Attachment A;
- i. Any communications with others regarding the use of or concealment of covert recording devices;
- j. Evidence of user attribution showing who used or owned the Apple accounts listed in Attachment A at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

ATTACHMENT C

Code Section

Offense Description

18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2251(a) and (e)	Production of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the Riverside (Ohio) Police Department and FBI, I am currently involved in an investigation of child exploitation offenses committed by JEREMY WELLS (hereinafter referred to as "WELLS"). This Affidavit is submitted in support of an Application for a search warrant for the following:
 - a. Information associated with the Apple ID jwellz1987@gmail.com and DSID¹ **11069587135** that is stored at premises controlled by Apple Inc. (as more fully described in Attachment A).
3. The purpose of the Application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography, and 18 U.S.C. §§2251(a) and (e), which make it a crime to produce or attempt to produce child pornography. The items to be searched for and seized are described more particularly in Attachment B hereto.
4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the search of the above noted account (as described in Attachment A).
6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), and 2251(a)

¹ Destination Signaling Identifier (DSID) is a unique identification number assigned to each user when registering at iCloud.com.

and (e) are present within the information associated with the above noted account (as described in Attachment A).

JURISDICTION

7. This court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

8. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
9. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.
10. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or

transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

BACKGROUND INFORMATION

Definitions

11. The following definitions apply to this Affidavit and Attachment B to this Affidavit:
- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).
 - e. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- f. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- g. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- h. **“Wi-Fi”** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.
- i. A **“wireless telephone”** (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- j. A **“digital camera”** is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- k. A **“GPS”** navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated **“GPS”**) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- l. A **“flash drive”**, also commonly known as a thumb drive, pen stick, gig stick, flash stick, jump drive, memory stick, and USB stick, is a data storage device that includes flash memory with an integrated USB interface. A flash drive is typically removable, re-writable, and much smaller than an optical disk.
- m. A **“Secure Digital Card”** or **“SD Card”** is a non-volatile memory card for use in portable devices, including cellular telephones. SD cards are available in three different sizes – original size, mini size, and micro size.
- n. A **“SIM Card”**, **“subscriber identity mobile card”**, or **“subscriber identification mobile card”** is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephone devices. It may store other information, including telephone number, contact lists, and text messages.
- o. An **“xD-Picture Card”** or **“eXtreme Digital Card”** is a flash memory card format used in digital cameras.
- p. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks,

printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Use of Computers and the Internet with Child Pornography

12. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.
 - a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.
 - b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to

engage in mutual validation of their interest in such material through Internet-based communications.

- c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.
- d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Apple ID's and iCloud

- 13. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.
- 14. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:
 - a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
 - b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages

("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
 - d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.
 - e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
 - f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.
 - g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
 - h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.
15. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

16. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.
17. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.
18. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.
19. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

20. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.
21. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.
22. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.
23. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. This location information is materially relevant to investigations involving interstate travels (such as stalking), weapons offenses, kidnapping, and other related offenses in that it helps to identify the subjects' travels and whereabouts at the times of the criminal offenses.

24. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

FACTS SUPPORTING PROBABLE CAUSE

25. On or around June 11, 2018, an adult female who will be referred to for purposes of this Affidavit as "Adult Female A" contacted the Riverside Police Department. Adult Female A reported suspicions that her husband, WELLS, had been videotaping her 12-year old daughter in the bathroom. Adult Female A was interviewed by a Sergeant of the Riverside Police Department and provided a written statement. In summary, Adult Female A provided the following information:
- a. Adult Female A and WELLS resided at 827 Sagamore Avenue in Riverside, Ohio along with three children: Adult Female A's 12-year old daughter who will be referred to for purposes of this Affidavit as "Minor A", Adult Female A's 11-year old son who will be referred to for purposes of this Affidavit as "Minor B", and Adult Female A's and WELLS's five-year old son who will be referred to for purposes of this Affidavit as "Minor C".
 - b. In the past two to three months, WELLS had become very protective of Minor A. He frequently took her places by herself (such as to gas stations) and bought her food (such as candy and iced coffees). WELLS also frequently looked through Minor A's phone, sometimes "obsessively" for hours. WELLS sometimes posed as Minor A and sent text messages to boys who she was communicating with, telling them that she did not want to be their girlfriend or making other rude comments.
 - c. Earlier that day (June 11, 2018), Minor A went into the bathroom to take a shower. Minor C went into the bathroom during that time period to use the toilet, and WELLS went in to assist Minor C. WELLS later claimed that he had a stomach ache and went back into the bathroom while Minor A was still in the shower. WELLS was behaving unusually that morning.
 - d. Around 1:00 p.m., Adult Female A took WELLS to his place of employment in Huber Heights, Ohio. After Adult Female A returned to the residence, Minor B told her that WELLS had called and asked Minor B to hide WELLS' hair clippers from her. Minor B showed Adult Female A where the clippers were located. In the tote or container for these clippers, Adult Female A found an empty toilet paper roll that was flattened out and had a hole cut in it. The guards for the clippers were shoved into each end of the toilet paper roll. Adult Female A

removed the guards and found WELLS' iPod inside of the toilet paper roll.

- e. Adult Female A advised that the iPod was used exclusively by WELLS, and it required a password to access it. Adult Female A was able to guess the password and view the contents of the iPod. Adult Female A observed approximately three videos from the present date (June 11, 2018) and one video from a separate date, all of which contained recordings of the bathroom in her home. Adult Female A noted that two of the videos (one from the present date and one from a prior date) depicted Minor A undressing to the point of nudity and getting into and out of the shower. Adult Female A further noted that the video from the present date that depicted Minor A undressing also depicted Minor C using the bathroom.
 - f. After finding the videos, Adult Female A called WELLS and questioned him about the videos. At that time, WELLS denied making the videos. Adult Female A thereafter received a text message from WELLS in which he stated that he would kill himself if she "labeled" him. Approximately one hour later, Adult Female A received another text message from a telephone number utilized by WELLS' boss. This text message appeared to be from WELLS, and it stated: "So am I on the run?" (or words to that effect).
 - g. Adult Female A also reported a recent incident in which she was physically assaulted by WELLS.
 - h. Adult Female A reported that over the past few months, she developed suspicions that WELLS was cheating on her with other women and using drugs.
26. Adult Female A voluntarily turned over WELLS' iPod to the Riverside Police Department. It was determined that this iPod contained a serial number of CCQT64E8GGK6.
27. Later on or around June 11, 2018, officers of the Huber Heights (Ohio) Police Department located WELLS at his place of employment and arrested him for misdemeanor domestic violence. This arrest was based on the information provided by Adult Female A about being physically assaulted by WELLS (as detailed above). Pursuant to the arrest, a ZTE cellular telephone was located on or near WELLS' person and was collected by the Huber Heights Police Department. The cellular telephone was subsequently turned over to the Riverside Police Department.
28. On or around June 12, 2018, a search warrant was authorized by the Montgomery County (Ohio) Common Pleas Court authorizing the searches of WELLS' iPod and ZTE cellular telephone. Initial examinations were conducted of these devices on or around June 12 and 13, 2018. Based on technical problems encountered during the forensic examination process, a second search warrant was authorized by the United States District Court for the Southern District of Ohio on or around June 22, 2018, authorizing the additional

searches of the devices.

29. During the examinations of the iPod, three videos were located that appeared to be surreptitious recordings of the bathroom in WELLS' residence. Below is a summary of these recordings:
- a. IMG_4050.MOV: The video depicted Minor A undressing and getting into the shower. The camera was set to directly capture the shower. While Minor A was standing in close proximity to the camera, and while the camera was focused on the mid-section of her body, Minor A briefly spread apart her vagina. The video was approximately three minutes and twenty-eight seconds in duration. Metadata for the file identified that the video was created on or around May 14, 2018 at 10:40 p.m. using an Apple iPod Touch.
 - b. IMG_4059.MOV: The video depicted WELLS flushing the toilet and adjusting the camera. The camera was initially set to capture both the toilet and shower. WELLS later entered the bathroom and adjusted the camera so that it directly captured the shower. No other individuals were captured in the recording. The video was approximately fourteen minutes and thirty-two seconds in duration. Metadata for the file identified that the video was created on or around June 11, 2018 at 11:29 a.m. using an Apple iPod Touch.
 - c. IMG_4060.MOV: The video began by depicting WELLS looking into and adjusting the camera. The camera was set to directly capture the shower. The video depicted Minor A, two minor males (believed to be Minor B and Minor C), and Adult Female A using the toilet. Minor C's penis was briefly exposed to the camera. The video depicted Minor A undressing, getting into and out of the shower, and re-dressing. While Minor A was both undressing and re-dressing, she was in close proximity to the camera and the camera was focused on the mid-section of her body. During those times, Minor A's vagina was exposed to the camera. Also during the video, WELLS entered the bathroom on two occasions – on one occasion to help Minor C on the toilet, at which time he looked directly into the camera and then adjusted the camera in what appears to be an attempt to better conceal it, and on another occasion to bring a shirt to Minor A. At the end of the video, Minor B entered the bathroom and removed the camera. The video was approximately one hour, twenty-three minutes, and forty seconds in duration. Metadata for the file identified that the video was created on or around June 11, 2018 at 12:03 9.m. using an Apple iPod Touch.
30. The examination of the iPod also determined that the device was associated with the Apple ID of jwellz1987@gmail.com, and that there was an iCloud account established on the device.
31. A preliminary examination has been conducted of the ZTE cellular telephone. No images or videos depicting child pornography were recovered during this preliminary

examination.

32. Following his arrest for misdemeanor domestic violence, WELLS was incarcerated at the Montgomery County (Ohio) Jail during the approximate time period of June 11 to 12, 2018. During this time period, WELLS made telephone calls from the jail's recorded telephone system. Review of the telephone calls provided the following information:

- a. On or around June 12, 2018, WELLS called Adult Female A. During this telephone call, WELLS inquired if Adult Female A gave anything to the Riverside Police Department (presumably referring to his iPod). Adult Female A told WELLS that she found the recordings of Minor A and gave the iPod to law enforcement officers. WELLS became upset and expressed concerns about his potential incarceration. Below are excerpts of the conversation:

WELLS:	Did you give them anything?
Adult Female A:	What do you mean?
WELLS:	Riverside.
Adult Female A:	Did I give them what?
WELLS:	Anything.
Adult Female A:	Why, why are you worried about that?
WELLS:	Because if you did, I'm going for eight years.
Adult Female A:	Oh why, because you been buying guns off of Mohammad?
WELLS:	No.
Adult Female A: That's the least of my worries. Yeah, they got your iPod. Are you kidding me? I found videos you took of my naked daughter, you sick fuck.
WELLS:	[Unintelligible]
Adult Female A:	Hell yeah I gave it to them. I saw you wipe [Minor C's first name] ass then bend down and adjust the camera. Hell yeah I saw it, you weren't recording yourself cutting your hair.
WELLS: You really should have thought about that.
Adult Female A:	I should have. What should I, how, in what way?
WELLS:	You gonna take me out of my son's life for that long?
Adult Female A:	Do you think I give a fuck?
WELLS:	No.
WELLS: You have to, I'm dying. Like, if I have to do eight years, I'm not coming out.
Adult Female A:	I can't hear you.

WELLS: If I got to do eight, I'm not coming out.
.....
Adult Female A: You need to tell your mother what you did.
WELLS: What do you mean I did? I've already talked to my mom.
Adult Female A: No, you told your mom you were recording yourself cutting your hair and it was an accident. And you clearly can see that that was no fucking accident. And it wasn't an accident about two weeks ago either.
WELLS: Listen, you gave them that for real?
Adult Female A: Yeah, did you hear me? What do you think I did?
WELLS: [Unintelligible] Look.
Adult Female A: What do you think I did?
WELLS: That's one of the most important things that I need to know because.
.....
Adult Female A: I sat at the police station for what, five hours yesterday.
WELLS: And you, you gave them that?
Adult Female A: What do you think I did?
WELLS: [Unintelligible]
Adult Female A: What do you think I did? You think I'm going to walk in there and just tell them that I found it and say I got rid of it?
WELLS: You know, I'm gone.
.....
Adult Female A: I just want my life back.
WELLS: So do I.
Adult Female A: I want you back the way you were.
WELLS: It's that stuff. And when I'm not recorded I'll explain it.
.....
Adult Female A: I don't know why you would do that. I don't know why you would mess up our family. I don't know why you would do that to [Minor A's first name]
WELLS: Listen, from me to you, if I have to do, if I'm in here, I'm not, I'm not doing it, like for real.
.....
Adult Female A: They just got your search warrant this morning [Unintelligible] since I've been on the phone with you.
WELLS: What?
Adult Female A: They just got the search warrant.
WELLS: Oh that's wonderful. God damn, god damn, god

Adult Female A: damn, god damn.
 [Unintelligible] I want what's best for everybody, I don't.
 WELLS: I'm gone [Adult Female A's first name], gone.

 WELLS: [Unintelligible], gone.
 Adult Female A: I just want to know why?
 WELLS: Cause, they're gonna look at that, I'm already, I'm already a.
 Adult Female A: No, I, I said why, I mean why would you do that?
 WELLS: I don't know.
 Adult Female A: [Unintelligible] head?
 WELLS: Huh?
 Adult Female A: What was going through your head?
 WELLS: I don't know.

 WELLS: But please, please do something. This is the end of my life here man. Like really.

- b. On or around June 12, 2018, less than one hour after calling Adult Female A, WELLS called a female who appeared to be his mother. The female told WELLS "I hope it don't go any farther" (presumably referring to WELLS' current charges). WELLS responded with the following: "Well [Adult Female A's first name] turned my shit in, they're going to get something else, which is bullshit. I need to go, I'm flipping out."
33. On or around June 13, 2018, Minor A was interviewed by an individual trained in conducting forensic interviews of children. Minor A provided the following information during the interview:
- a. Minor A described WELLS as being her "best friend". She said that they talked about everything, got ice cream together, and drove around the neighborhood together.
 - b. Minor A thought that WELLS recently was acting weird and secretive.
 - c. Minor A stated that although her brothers were allowed to use WELLS' iPod, he did not allow her to use it. WELLS told her that there were things on the iPod that she was not supposed to see.
 - d. On the morning that Adult Female A found the iPod in the bathroom, WELLS was behaving unusually. He kept coming into and out of the bathroom. Minor A was not aware that WELLS was recording her.

- e. Minor A heard WELLS call Adult Female A after Adult Female A found the iPod. Minor A heard WELLS claim that he hid the iPod in the bathroom because he thought that someone was living in the attic.
34. WELLS was released from the Montgomery County (Ohio) Jail from his domestic violence arrest on or around June 12, 2018. WELLS was arrested pursuant to a federal complaint and arrest warrant for two counts of production of child pornography (in violation of 18 U.S.C. §§2251(a) and (e)) on or around June 28, 2018. He has been incarcerated at the Shelby County (Ohio) Jail since on or around June 29, 2018.
35. In July and August 2018, I interviewed Adult Female A on a number of occasions. Below is a summary of some of the information provided by Adult Female A during the various interviews:
- a. After WELLS was released from jail for his domestic violence offense, he told Adult Female A that he surreptitiously recorded Minor A in the bathroom to find evidence if she was cutting herself. WELLS claimed that he had in fact captured at least one recording of Minor A cutting herself.
 - b. WELLS' mother told Adult Female A that WELLS claimed that he inadvertently recorded Minor A in the bathroom when he was trying to record himself cutting his hair.
 - c. Adult Female A initially believed WELLS' explanation that he surreptitiously recorded Minor A in the bathroom to find evidence if Minor A was cutting herself, and Adult Female A reconciled with WELLS. While she supported him for some time, she later developed doubts and no longer believed his explanations.
 - d. During the time period that Adult Female A was communicating with WELLS via the jail's telephone system, there were a number of occasions when he asked her to tell investigators that she knew he was recording Minor A in the bathroom. WELLS also told Adult Female A to tell investigators that she was under the influence of drugs when she found the iPod. Adult Female A advised that this was not true, and that she did not know that WELLS was recording Minor A until she found the iPod in June 2018. Adult Female A also advised that WELLS and his family members pressured her on numerous occasions to write a letter stating that she knew about the recordings. Although Adult Female A did not know about the recordings, she ultimately wrote the letter due to the pressure she was receiving. Adult Female A also felt intimidated by WELLS' family members, and she had concerns that they had intentionally damaged the tire on her car when she was at WELLS' mother's residence. Adult Female A stated that she regretted writing the letter.
 - i. After receiving the information about the damaged tire from Adult Female

A, I drove by WELLS' mother's residence. Consistent with the information reported by Adult Female A, I observed the vehicle that Adult Female A is known to drive parked in the driveway with a flat tire.

- e. Adult Female A stated that WELLS only had the ZTE cellular telephone that was seized by the Riverside Police Department (as detailed above) for a short period of time. Adult Female A could not recall what happened to the previous telephone that WELLS utilized.
- f. Around May or June 2018, WELLS ordered a government-subsidized QLink Wireless cellular telephone. WELLS allowed Minor C to use the telephone for a short period of time before WELLS began using it in addition to WELLS' other telephone. Adult Female A noted that Minor C sometimes referred to WELLS' QLink Wireless telephone and WELLS' iPod as his (Minor C's) telephones.
- g. On one occasion, Adult Female A accessed WELLS' cellular telephone and saw that he had been viewing pornography depicting young teenagers.
- h. Approximately one year ago, WELLS showed Adult Female A a video he had on either his cellular telephone or iPod that depicted Minor B masturbating in the bathroom. WELLS told Adult Female A to talk to Minor B about the masturbation. Adult Female A saw that the video was still on WELLS' cellular telephone or iPod approximately one week later. She questioned WELLS about why the video was still on the device, and he claimed that he forgot about it.
- i. Around the summer of 2016, Minor A's friend told Adult Female A that she (the friend) found a camera in Minor A's bedroom. Sometime shortly thereafter, Adult Female A found a small camera in Minor A's bedroom window. After finding the camera, Adult Female A questioned WELLS about the camera. WELLS claimed that he was trying to set up a "nanny camera" to determine if Minor B was bullying Minor C. WELLS told Adult Female A that the camera's footage could be viewed on his cellular telephone through an application, and that he could take still images of the footage.
- j. Beginning in mid-August 2018, Minor C has told Adult Female A on several occasions about pictures and videos he found on his telephone that depicted Minor A naked. Adult Female A believed that Minor C was referring to WELLS' QLink Wireless cellular telephone and/or iPod when referring to this phone. Adult Female A's mother informed me that she heard one of these conversations. According to Adult Female A, the information Minor C relayed to her about these pictures and videos included the following:
 - i. Minor C originally told Adult Female A that he found two pictures or videos that depicted Minor A nude on his phone – one that depicted her

nude in the bathroom and one that depicted her nude in her bedroom. Minor C observed WELLS setting up a camera in the bathroom on one occasion. Minor C said that after he saw the pictures and videos, he hid in his closet and deleted the files. Minor C told WELLS that he saw the pictures and videos of Minor A, and WELLS performed a factory reset on the phone. WELLS also told Minor C not to tell Adult Female A about the pictures and videos.

- ii. Minor C also talked about a time when he went into the bathroom and saw a black camera and a telephone (presumably preferring to WELLS' cellular telephone or iPod) on a shelf on or in white buckets with black stickers. Minor C said that he retrieved the telephone and took photographs of himself with the device. When he tried to access the photographs he took of himself, he saw approximately seven pictures and videos that depicted Minor A nude in the bathroom. Minor C said that he again deleted the files after viewing them.

- 1. Adult Female A was familiar with the white buckets with black stickers that Minor C referenced. Adult Female A advised that she purchased these buckets and stickers around the Easter holiday of 2018.

- k. After WELLS' arrest, Adult Female A moved into a different residence. She put a number of her belongings into the shed at this new residence. On or around August 20, 2018, Adult Female A went into the shed and saw that the side pocket of a camera case belonging to her deceased father was bulging. This camera case had particular sentimental value to Adult Female A, and she had not accessed it in a while. Adult Female A noted that her family members were aware of the camera's sentimental value and were not supposed to use it. Adult Female A looked in the pocket and found approximately twenty-four electronic devices, to include an iPod, a cellular telephone, approximately three digital cameras, and a number of flash drives, picture cards, micro SD cards, SIM cards, and SD adapter cards. These items did not belong to her deceased father, nor did Adult Female A put the items there. Adult Female A provided the following additional information regarding these items:

- i. Adult Female A recognized the cellular telephone (a QLink Wireless cellular telephone) to be the government-subsidized cellular telephone that WELLS purchased around May or June 2018.
 - ii. Adult Female A recognized one of the digital cameras (an HD Microsoft camera) to be the camera she observed in Minor A's bedroom window during the summer of 2016.
 - iii. A number of other electronic devices (including flash drives, picture cards,

micro SD cards, SIM card, and SD adapter cards) were contained in a small red Tupperware container. Adult Female A recalled finding this Tupperware container in WELLS' pants' pocket sometime in the past. WELLS claimed at that time that the container held SD cards that had pictures of his deceased step-father.

- iv. Adult Female A showed one of the digital cameras (the Sony Cyber-shot camera) to Minor C but did not ask him any questions. Minor C immediately stated that this was the camera he saw in the bathroom on or in the white buckets with black stickers.
36. Adult Female A voluntarily turned over the above noted devices to me on or around August 21, 2018. A search warrant was subsequently authorized by the United States District Court for the Southern District of Ohio authorizing the searches of these devices. The searches of the devices are currently in-progress.
37. On or around August 14, 2018, Minor C was interviewed by an individual trained in conducting forensic interviews of children. Minor C was difficult to understand at various times during the interview. He also became emotional at one point in the interview, and the interview was terminated shortly thereafter. Minor C provided the following information during the interview:
- a. Minor C stated that he had observed two pictures and one video that depicted Minor A nude on what he referred to as his iPhone. Minor C indicated that one of the images and the video depicted Minor A in the bathroom, and one of the images depicted her in her bedroom. Minor C stated that the video was "nasty".
 - i. As detailed above, Adult Female A stated that Minor C referred to WELLS' iPod and QLink Wireless cellular telephone as his (Minor C's) telephones. As such, it appears that Minor C was likely referring to WELLS' iPod.
 - b. Minor C saw WELLS set up a camera in the bathroom on one occasion.
 - c. WELLS told Minor C not to talk about the pictures and video of Minor A.
38. It should be noted that the interview of Minor C occurred before he told Adult Female A that he found the camera and telephone in the bathroom on or in the white buckets with black stickers. The interviewer therefore did not ask Minor C about this incident.
39. On or around November 18, 2018, Adult Female A contacted me regarding files she found earlier that day in WELLS' iCloud account. Below is a summary of information provided by Adult Female A:

- a. Adult Female A recently developed suspicions that someone had stolen her identity and opened accounts in her name. She also developed suspicions that WELLS might have been involved in this possible identity theft.
 - b. Adult Female A knew that WELLS had an iCloud account associated with the Apple ID of jwellz1987@gmail.com (consistent with the information obtained during the examination of WELLS' iPod, as detailed above). Adult Female A wanted to check WELLS' iCloud account to see if he was involved in creating the possible accounts that were opened in her name.
 - c. On or around November 18, 2018, Adult Female A was able to reset the password to WELLS' iCloud account (containing the Apple ID jwellz1987@gmail.com) and access its contents. Consistent with her suspicions, Adult Female A found pictures of her and her step-father's drivers' licenses in the iCloud account.
 - d. Adult Female A also viewed the preview thumbnail images² of some of the video files stored in WELLS' iCloud account. Adult Female A found that a number of the videos appeared to depict Minor C. However, Adult Female A did not recognize one of the preview thumbnail images and opened the video file. Adult Female A found that the video depicted WELLS setting up a camera in the bathroom of her previous residence. Adult Female A saw that Minor A then entered the bathroom, undressed to the point of nudity, and got into the shower. Adult Female A fast forwarded the video until she saw Minor A get out of the shower, get dressed, and exit the bathroom. Adult Female A then saw WELLS enter the bathroom. WELLS turned on the sink faucet and retrieved the camera. Adult Female A noted that WELLS had what appeared to be a live lizard on his arm. Adult Female A also noted that the video was dated on or around May 2, 2018.
 - e. After viewing the video of Minor A in the bathroom, Adult Female A did not look at any additional videos or images in the iCloud account. Adult Female A logged out of the iCloud account, and she has not accessed it since that time.
40. Based on the apparent file date of the video observed by Adult Female A in WELLS' iCloud account, as well as the presence of the apparent lizard on his arm (which was not observed in the video files recovered from WELLS' iPod, as detailed above), it is reasonable to believe that the iCloud account contains one or more surreptitious video files depicting Minor A which was (were) not recovered from the iPod. Based on my training and experience, I know that files deleted from an Apple device may still be present in their iCloud account if the device was backed up to the iCloud before the files were deleted on the device.

² When viewing video files in Windows explorer, individuals can view thumbnail images that depict the opening scene of the videos.

41. On or around July 17, 2018, an administrative subpoena was served to Apple Inc. requesting subscriber information, IP logs, and transactional records for any Apple accounts associated with the Apple ID of jwellz1987@gmail.com. Records received from Apple Inc. in response to the subpoena identified that an iCloud account associated with the Apple ID of jwellz1987@gmail.com and a DSID of **11069587135** was established on or around April 27, 2017. The iCloud account was associated with two devices: an iPod Touch bearing serial number CCQT64E8GGK6 and an iPhone 5S bearing serial number F2LMRM8VFFDR.
- a. The serial number for the iPod Touch matches the serial number of the iPod seized by the Huber Heights Police Department, which contains the three surreptitious recordings of the bathroom in WELLS' residence (as detailed above).
 - b. As detailed above, Adult Female A advised that WELLS only had his ZTE cellular telephone for a short period of time, but that she could not recall the make or model of his previous telephone. Based on the records obtained from Apple Inc., it is reasonable to believe that the iPhone 5S that was associated with the jwellz1987@gmail.com iCloud account may have been WELLS' previous cellular telephone.
42. Since the time of WELLS' arrest, I have monitored some of the calls he has made from the jail's recorded telephone system. Due to the large number of calls that WELLS has made, I have only listened to a small sample of calls. The below information was noted from the telephone calls that have been monitored to-date:
- a. Consistent with the information provided by Adult Female A, there were at least three telephone calls when WELLS pressured her to tell investigators that she knew about the recordings of Minor A and that she was under the influence of drugs when she found the iPod. WELLS claimed that his attorney told him that the charges would be dismissed if Adult Female A told this to investigators. On two of these telephone calls, WELLS prefaced the conversations by instructing Adult Female A not to respond to anything he was saying.
 - b. During several telephone calls, WELLS told Adult Female A that she needed to "do something" to get his charges dismissed.
 - c. Consistent with the information provided by Adult Female A, there were telephone conversations when Adult Female A talked about the damage to her vehicle's tire and her suspicions that WELLS' family members were involved in causing the damage. During a later telephone conversation with his aunt, WELLS told the aunt not to fix Adult Female A's vehicle until after he got out of jail.
 - d. During a visitation with his aunt on or around August 6, 2018, the aunt told

WELLS to stop talking to Adult Female A. There were various periods of time when WELLS and the aunt were whispering and/or possibly mouthing words to each other or passing notes, as they became inaudible and difficult to understand. However, WELLS and the aunt were briefly heard talking about the whereabouts of WELLS' "Obama" phone (a common term to refer to government-subsidized cellular telephones such as the QLink Wireless telephone). WELLS was next heard briefly asking if "they" (possibly referring to law enforcement officers) had spoken to Minor C.

- i. Based on my training and experience, I know that individuals who are incarcerated often try to evade the jail's recording system of their telephone calls and visitations when discussing incriminating matters. These evasion techniques commonly include speaking in code, whispering, mouthing words, and/or passing notes.
43. Based on the information noted in the Affidavit, there is probable cause to believe that WELLS produced or attempted to produce child pornography depicting Minor A, Minor B, and/or Minor C. At least two of the videos were produced utilizing an iPod.
44. Again based on all of the information noted in the Affidavit, it is reasonable to believe that WELLS produced and possessed more videos depicting child pornography than the two videos recovered from his iPod (which are detailed above). It is reasonable to believe that WELLS may have produced surreptitious videos depicting Minor A and Minor B beginning in at least 2016 (the time at which Adult Female A found the camera in Minor A's bedroom), and that he continued producing such videos at various times continuing thereafter. Based on the video file that Adult Female A viewed in WELLS' iCloud account (as detailed above), there is probable cause to believe that one or more surreptitious videos of Minor A produced by WELLS (which depict child pornography) is (are) contained in his iCloud account containing the Apple ID of jwellz1987@gmail.com and DSID **11069587135**.

Evidence Available on iCloud Accounts

45. Based on the information detailed above, I believe that the iCloud account containing the Apple ID of jwellz1987@gmail.com and DSID **11069587135** is associated with WELLS' iPod and potentially his iPhone 5S. As detailed above in the background section of the Affidavit, Apple's iCloud service provides the means to wirelessly back up iOS devices directly to iCloud instead of being reliant on manual backups. As such, data stored on cellular telephones, iPads, and other Apple devices can be stored on and recovered from the users' iCloud accounts.
46. Based on my training and experience, I know that individuals are increasingly utilizing cellular telephones, iPods, and tablets to do their computing. In my experience, I know that individuals involved in child pornography offenses often utilize both computer devices and their cellular telephones to obtain and store their child pornography files.

Due to their portable nature, cellular telephones provide individuals easy access to their files.

47. In my experience, I know that due to the covert nature of the devices, individuals involved in child pornography offenses also utilize their cellular telephones to take photographs of children and produce child pornography. Based on my training and experience and examination of similar devices, I know that most cellular telephones have digital cameras. Examination of the exterior of the iPod seized from WELLS' residence indicates that it does in fact have a camera. Based on my training and experience, I know that iPhone 5S cellular telephones also have cameras.
48. Again based on my training and experience and examination of similar devices, I know that many cellular telephones have the ability to connect to the Internet. I also know that many cellular telephones provide users with the ability to send and receive email messages. Individuals involved in child pornography offenses often utilize their cellular telephones to access Internet websites, exchange email messages, and access social media accounts to search for, view, and download child pornography.
49. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
50. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel their victims to engage or continue engaging in the illicit sexual activities (including the production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.
51. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chat rooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

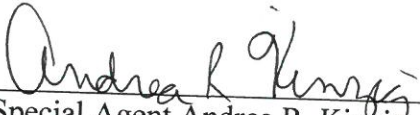
52. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the offenders' cellular telephones.
53. In my experience, I know that many cellular telephones store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during their criminal activities.
54. As detailed above, various other subscriber information, device activation information, sign-on logs, and transaction data are maintained by Apple Inc. for its products and applications. Such information is often materially relevant in child pornography investigations in that it helps in identifying the subjects and the locations where their computer devices are located.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

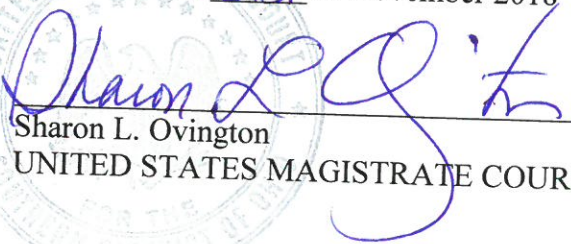
55. I anticipate executing the requested warrant for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple Inc. to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

56. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located in the account described in Attachment A: 18 U.S.C. §§2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), and 2251(a) and (e).
57. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.
58. Because the warrant for the account described in Attachment A will be served on Apple Inc., who will then compile the requested records at times convenient to that entity, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 21st of November 2018


Sharon L. Ovington

UNITED STATES MAGISTRATE COURT JUDGE